(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 292 790**
A3

(12) EUROPEAN PATENT APPLICATION

(21) Application number: **88107596.4**

(51) Int. Cl.4: **H04L 9/00**

(22) Date of filing: **11.05.88**

(30) Priority: **29.05.87 US 55502**

(43) Date of publication of application:
30.11.88 Bulletin 88/48

(84) Designated Contracting States:
DE FR GB IT NL

(88) Date of deferred publication of the search report:
24.01.90 Bulletin 90/04

(71) Applicant: **International Business Machines Corporation**
Old Orchard Road
Armonk, N.Y. 10504(US)

(72) Inventor: **Matyas, Stephen Michael, Jr.**
8978 Miles Place
Manassa Virginia 22110(US)
Inventor: **Meyer, Carl Heinz Wilhelm**
27 Norma Court
Kingston New York 12401(US)
Inventor: **Brachtl, Bruno Oswald**
Weinbergstrasse 20
D-7033 Herrenberg(DE)

(74) Representative: **Grant, Iain Murray**
IBM United Kingdom Limited Intellectual Property Department Hursley Park
Winchester Hampshire SO21 2JN(GB)

(54) Controlling the use of cryptographic keys via generating station established control values.

(57) A method of controlling the use of securely transmitted information in a network of stations in which each potentially cooperating station includes a cryptographic facility (10) which securely stores a master key and in which, for each transmission between a pair of stations, a cryptographic key result is provided for each station of the pair by a generating station which is either one of the pair or a station external to the pair under a cryptographic protocol common to the network, the cryptographic key results for the transmission having a random component notionally particular to the transmission, a master key variant component characteristic of the protocol and a target station component either particular to the stations individually or as a pair, wherein, in response to a generating command invoked in the generating station for establishing a controlled use secure transmission between a designated pair of stations, the generating station generates the cryptographic key result for each designated station, accesses the control value common to the system for the permitted operation for each of the stations for the particular transmission, combines the control value with the common key result or each individual key result and causes the appropriate combined key result to be established in each station of the pair for the transmission, and wherein the cryptographic facility (10) in each station is arranged, when an operating command is invoked to perform a designated operation with respect to such securely transmitted information, to automatically abort such operation unless it matches the control value.

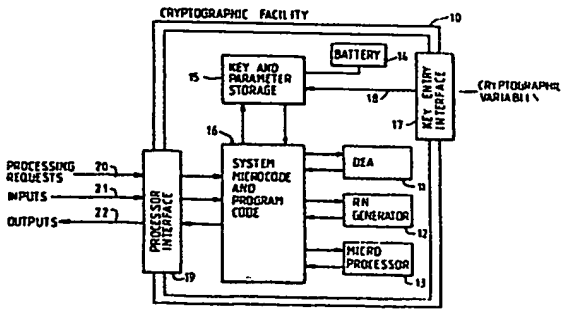

FIG. 2

European Patent Office

EUROPEAN SEARCH REPORT

Application number

DOCUMENTS CONSIDERED TO BE RELEVANT

EP 88107596.4

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.4)
D,A	US - A - 4 227 253 (EHRSAM et al.) * Abstract; column 11, line 15 - column 19, line 37; column 28, line 43 - column 34, line 68; fig. 1,2,17, 18 *	1,2,7, 13,17	H 04 L 9/00
A	US - A - 4 649 233 (BASS et al.) * Column 1, line 8 - column 3, line 12; column 3, line 28 - column 7, line 57; fig. 1-3 *	1,2,7, 13,17	
D,A	US - A - 4 386 233 (SMID et al.) * Abstract; column 1, line 30 - column 3, line 56; column 4, line 21 - column 9, line 55; fig. 1-6 *	1	
A	US - A - 4 578 530 (ZEIDLER) * Abstract; column 3, lines 17-35; column 3, line 52 - column 5, line 26; column 8, line 4 - column 10, line 66; fig. 1 *	1	TECHNICAL FIELDS SEARCHED (Int. Cl.4) H 04 L G 06 F
A	WO - A1 - 81/02 655 (SENDROW) * Page 5, line 21 - page 7, line 29; page 8, line 18 - page 13, line 13; fig. 1,2 *	1	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
VIENNA	10-11-1989	HAJOS

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO Form 1503. 03.82